International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 3, Jun 2014, 7-14
© TJPRC Pvt. Ltd.

STUDIES OF PROMINENT DoS ATTACKS IN THE INTERNET: THEIR CAUSES, PREVENTIONS AND CASE STUDIES

JOVI D'SILVA[1], KUKATLAPALLI PRADEEP KUMAR[2] & BALACHANDRAN K[3]

[1]M.Tech Student, Department of Computer Science and Engineering, Christ University, Faculty of Engineering, Mysore, Bangalore, Karnataka, India

[2]Assistant Professor, Department of Computer Science and Engineering, Christ University Faculty of Engineering, Mysore, Bangalore, Karnataka, India

[3]HOD, Department of Computer Science and Engineering, Christ University Faculty of Engineering, Mysore, Bangalore, Karnataka, India

ABSTRACT

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) which has become a major concern in cyber security now, can be seen as a trial to make a computer or network resource unavailable or occupied so that its intended users can not use it. In DoS attacks, the attackers usually aim at interrupting Internet services that are being availed by legitimate users. For this purpose, the networks and the victim systems are targeted and flooded in such a way that movement of legitimate traffic across the system becomes almost impossible. The increased traffic causes consumption of incoming bandwidth as well as outgoing bandwidth. In many of these attacks, the victim machines are completely clogged and saturated resulting in those systems crashing as well as clogging and overloading the servers. Usually DoS attacks involve important or widely used websites and web services. In this paper we will be discussing the various types of DoS attacks on the Internet taking into account some case studies and simple means of preventing such attacks.

KEYWORDS: Denial of Service, Attacks, Simulation, Emulation, Testbeds, TCP, Denial of Service Attacks, Low-Rate TCP-Targeted Attacks

INTRODUCTION

Denials of Service (DoS) attacks have become progressively more rampant in recent times. According to a Prolexic survey, during the fourth quarter of last year, Prolexic detected 45 percent more DDoS attacks compared to the similar period of 2010 and more than twice the number of attacks observed during the third quarter of 2011. The average attack bandwidth registered in the fourth quarter of 2011 was 5.2G bps (bits per second), 148 percent higher than what it was during the third quarter. The year over year increase for attack bandwidth in 2011 was 136 percent[*]. These attacks usually target the internet hardware and software facilities like inter-domain routing protocols, key backbones, and Domain Name System (DNS) causing significant damage, such as network partitioning; which means disrupting communication in between portions of networks in a way that one portion is not accessible to the other portions. Since Denials of service (DoS) attacks have become a major threat to current computer networks, in this paper, we are trying to understand some major DoS attacks in recent times for the purpose of studying how these attacks can cause major damage to networks and also we are trying to have a better understanding of DoS attacks and prevention of the same.

TYPES OF DoS ATTACKS

TCP SYN Flooding

DoS attacks involve taking advantage of network protocols that have state information associated with it, like TCP (Transaction Control Protocol). These protocols utilize a lot of resources in order to maintain stateful information. TCP SYN flooding is an attack on TCP, which has a wide impact as most Internet services utilize TCP. When a user tries to establish a TCP connection with a web-server, the user initiates by sending a SYN message to the web-server followed by the server acknowledging the request for connection by sending a SYN-ACK message back to the user. The user completes the connection initiation process by responding with an ACK message. This operation is known as a Three-way Handshake.

In this operation, an attacker sends an enormous sequence of SYN requests to a potential target web-server. This action causes the web-server to be overwhelmed with the volume of connection requests such that the resources of web-server are completely exhausted making the web-server unresponsive to its legitimate users. In the second phase of the attack, as the web-server tries to disseminate the pressure of the large volume of SYN requests, the attacker continues sending request packets but does not send the "ACK" back to the web-server. The result is that on one hand the workload of the server gets increasing while on the other hand the existing workload refuses to get processed as the connections are left half-opened and continuously consuming the web-server's resources. A legitimate user tries to connect but the server refuses to open a connection resulting in a denial of service.

ICMP Smurf Flooding

Normally to decipher whether a computer in the internet network is responding or not, an ICPM echo request packet is sent to the computer which after receiving the request packet, in return sends back an ICMP echo reply packet to acknowledge its presence on the network. Now, in a Smurf Attack, the attacking host sends a large number of such ICMP request packets to several computers in the network forging the victim's IP address as the source address using an IP Broadcast address. Though the firewall or router filters the packets being sent to a computer, if in this case the router or firewall is not able to sift these spoofed packets, they are broadcast to all the computers on the network. Then, by default most of the computers will respond to this action by sending back the reply packets to the source IP address, which in this case is the victim's computer. In case there are too many computers on the network, the victim's network will be flooded with ICMP echo reply packets and will therefore become congested and inoperable.

Buffer Overflow Attacks

Buffer overflow is an anomaly wherein a program while writing data to a buffer for the purpose of storage exceeds the storage space of that particular buffer. As a result of this, excess data that is transferred into this buffer overflows into adjacent buffer spaces thus corrupting the data that is already present in that particular buffer space. In case of a buffer overflow attack, the hackers launch malicious instructions written in a file into a computer to corrupt the system, knowing well that the data will cause a buffer overflow and release these malicious instructions into the computers instructions. Once the attack happens, the system becomes corrupt and is forced to run the arbitrary codes launched by the hacker thus allowing the hacker to take over the system that is being attacked. This attack allows the attacker to run remote shell on the computer being attacked and gives the hacker the same privileges that the system administrator has. This type of attack is especially common in case of programs using C and C++ programming languages that does not provides protection against accessing or overwriting data in any part of the memory.

Teardrop Attack

The Teardrop Attack is an old technique but it is still in use. In this type of attack, the attacker impedes the way in which stacks rebuild IP packet fragments. The attacker in this case sends fragmented IP packet to the targeted system, each chunk still retaining the original IP packet's header, and a field that tells the TCP/IP stack what bytes it contains. Normally, this information is used by the system to reassemble the packet back together again. In case of a Teardrop attack, the hacker forges the fragments in such a way that when the host system tries to reconstruct the fragmented IP packets, they overlap due to a bug in the TCP/IP reconstruction assembly and therefore the reconstruction fails. This causes the system to crash and thus Denial of Service happens. Most systems now know how to deal with Teardrops and a firewall can block Teardrop packets as it disregards all broken packets that it receives. However, if a large number of such packets are thrown at a system, it is still susceptible to crashes.

Many other variants such as Targa, SynDrop, Boink, Nestea Bonk, TearDrop2 and NewTear are available to accomplish this kind of attack.

UDP Flooding Attacks

The UDP Flooding Attack uses the User Datagram Protocol (UDP) to achieve Denial of Service. This type of attack is initiated by sending a large number of spoofed UDP datagram in IP packets with a forged source address to a random port of the targeted machine that is usually the echo port. On receiving these spoofed UDP packets, the immediate response of the victim system is to establish the application that is waiting at the destination port. When the system realizes that there is no application waiting at the destination, it replies with an ICMP Destination Unreachable packet to the spoofed source address, which therefore does not reach the hacking system at all. Thus if a large number of such UDP packets are delivered to a targeted system, it creates a huge load on the system and the network, thus making the system so slow that the victim is not able to work at all. This type of attack however does not give the hacker any privilege of gaining additional access.

Ping Flood Attack

This is one of the oldest and most easily executed Denial of Services. A ping flood is a simple DoS attack where the attacker preferably having a high-bandwidth connection as compared to a low-bandwidth connection that the victim is using, sends a huge number of ICMP Echo Request (ping) packets using flood option of ping, as fast as possible to the victim system without waiting for replies. The victim system then has to acknowledge the ICMP Echo Request packets by sending back ICMP Echo Reply packets. The number of ICMP request packets is so enormous that the victim computer becomes overwhelmed with the number of requests and the need to send back so many reply packets. The result of the flood of ping packets over the network is that the movement of legitimate traffic over the network becomes limited and slow. This results in consumption of both outgoing as well as incoming bandwidth due to saturation of the network.

Ping of Death

This type of attack is easy to implement, as the hacker does not need any extra information apart from the IP address of the victim system. In this the attacker sends a distorted or harmful ping to a computer. The size of a ping packet is 56 bytes or if the IP protocol is considered then it can go up to 84 bytes. Usually computers cannot handle a ping packet larger than the maximum IPv4 packet size, which are 65,535 bytes, which is also the maximum size that an IP allows. The packet that the attacker sends is usually of a size larger than 65,535 bytes, which is too large to be sent in one packet, and therefore is fragmented which is allowed under TCP/IP (according to which packets are broken up into smaller chunks essentially reassembled when received). The attackers take advantage of this attribute and fragment packets in such a way that they add up to a greater file size (much more than 65,535 bytes) when eventually reassembled. This then leads to overflowing of the buffer thus causing the system to crash. This kind of attack was very common earlier since the chances of success were very high.

Distributed DoS Attacks (DDoS)

All the above types of Denial of Service attacks have a single attacker but in case of a Distributed DoS Attack, multiple compromised systems infected with Trojan Virus are used to target a single system. These infected systems are called "zombies" as they are completely controlled by the hackers. The main weapon for this kind of attack is bulk flooding where the multiple compromised system floods the victim computer with traffic. In case of distributed attacks, it is easier to generate more traffic over the server than one single compromised computer. The flood of incoming traffic into the victim's computer forces the computer to become slow and shut down eventually. The other advantage for the attacker is that it is difficult to track multiple compromised systems. In this case, major damage is done in a short span of time.

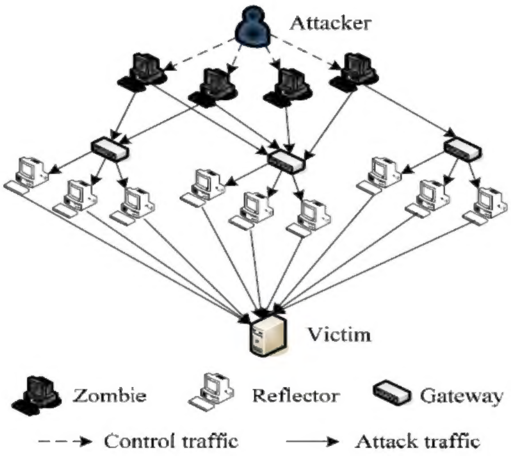

Figure 1: Distributed DoS

MEANS OF PREVENTION

There is a saying that prevention is always better than cure, following are some rules of thumb to follow in order to prevent the occurrence of a possible DoS attack.

- Planning is a very important step, because a well-planned system will have all possible considerations of security kept in mind and thus ensuring a more secure system overall.
- Conducting a cost study of the amount of investment that has been made in the system. Also investing in better, more specialized and secure networking hardware can help.
- Analyzing the system is very important for checking if there is a chance of an attack and making sure that the best possible security measures are implemented can also reduce the chance of attacks.

- Installing all available and necessary patches and updates of the software that are used on the network helps to protect the network from exploits which takes advantage of loopholes in application software.
- Disabling any unused or unnecessary network services or applications running in the foreground and the background can also ensure network security.

PROTECTING EXISTING NETWORKS

You must ensure the following steps to protect an already existing network from possible DoS attacks.

- Be vigilant and watch the network system, if any suspicious events occur on the network they must be made note of.
- Check the network configuration to make sure it is has been implemented correctly ensuring there are no loopholes for error.
- Maintain a recovery backup of the network so that the network can be restored in case it has suffered an extreme failure.
- Ensure that the password and the concerned backups that are taken of the network are consistent; if so this could be used to recover the network from a certain point after an attack.
- Trace any problem back to the source IP using some form of hybrid, trace back schemes and then on detection of the attacker move forward with legal and administrative actions.
- Disable features such as the ping protocol to help reduce risks of certain DoS attacks in the network.
- The use of a fully enabled and secured firewalls or a DMZ (De Militarized Zone) is used to ensure the safety of the sensitivity of the network behind it.

CASE STUDIES

Now we have considered some prominent case studies exemplifying the scale of damage possible with DoS attacks on the Internet.

Case 1

In July 2000, a vulnerability to buffer overflow attack was discovered in Microsoft Outlook and Outlook Express. A programming flaw made it possible for an attacker to compromise the integrity of the target computer by simply sending an e-mail message. Unlike the typical e-mail virus, users could not protect themselves by not opening attached files; in fact, the user did not even have to open the message to enable the attack. The programs message header mechanisms had a defect that made it possible for senders to overflow the area with extraneous data, which allowed them to execute whatever type of code they desired on the recipient's computers. Because the process was activated as soon as the recipient downloaded the message from the server, this type of buffer overflow attack was very difficult to defend. Microsoft has since created a patch to eliminate the vulnerability.

Case 2

Since Sept. 19 2012, the websites of Bank of, JPMorgan Chase, Wells Fargo, U.S. Bank and PNC Bank have all suffered daylong slowdowns and been sporadically unreachable for many customers. The attackers, who took aim at Bank of America, first, went after their targets in sequence. Security experts say the outages stem from one of the biggest cyber attacks they've ever seen. These "denial of service" attacks -- huge amounts of traffic directed at a website to make it crash To carry out the cyber attacks, the attackers got hold of thousands of high-powered application servers and pointed them all at the targeted banks.

Case 3

The Spamhaus Project is an international organization, based in both London and Geneva, founded in 1998 by Steve Linford to track email spammers and spam-related activity. The name spamhaus, a pseudo-German expression, was coined by Linford for an Internet service provider, or other firm, which spams or knowingly provides service to spammers. Spammers frequently respond to being listed with threats, legal action or denial-of-service attacks. The Spamhaus Project is responsible for compiling several very widely used anti-spam lists. Many Internet service providers and email servers use the lists to reduce the amount of spam they accept. The Spamhaus lists collectively protect over 1.77 billion email users, according to Spamhaus' web page (November 2012), and are estimated to block 80 billion spam emails per day globally on the Internet (almost one million per second).

Spamhaus distributes lists in the form of DNS-based Blocklists (DNSBLs) and Whitelists (DNSWLs). The lists are offered as a free public service to low-volume mail server operators on the Internet. Spamhaus was targeted with a massive cyber attack that experts say may have been the biggest in the history of the web. The dispute started when the spam-fighting group, called, added the Dutch company Cyberbunker to its blacklist, which is used by e-mail providers to weed out spam. The DDoS attack being waged against Spamhaus has reached a previously unheard of magnitude, 300gb/s (that's three hundred gigabits a second) of data. The massive cyber attack is apparently from groups angry at being blacklisted by the Geneva-based Spamhaus.

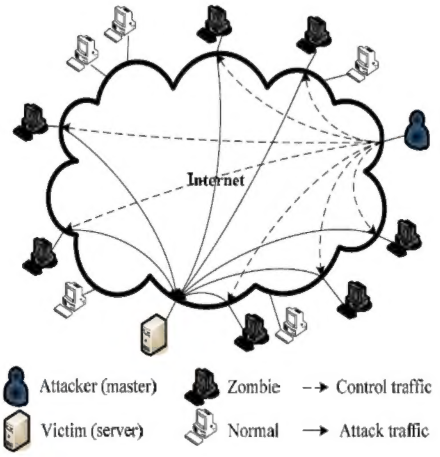

Figure 2: Wide Scale DDos on the Internet

CONCLUSIONS

After having discussed all the major DoS attacks, to conclude this paper we can say that in the Internet and any other large network, the routers are the weakest points which can be easily attacked and manipulated to send a large number of packets to all the hosts connected to it. Some of these packets can often be a part of a large or widespread distributed attack. Therefore it is important to secure the routers especially ones that act as an access point to the Internet.

The Internet is a very large network of computers and other devices making enforcement of counter mechanisms difficult. But at the same time, as the Internet is so large and since it is broken into distributed parts, on the other hand it is equally difficult for attacks to succeed completely as such attacks may not affect certain entities on the network at all. On the whole DoS attacks are possible on the Internet because of its magnitude but however it is sometimes very difficult to affect and undermine the entire working chunk of the Internet.

It can be said that a better way of dealing with DoS attacks is to prevent it from happening rather than recovering from DoS attacks. Also, constant monitoring can help to take action in case of absence of prevention and recovery techniques.

The attackers are ever evolving and so are their techniques. It can never be said that the system is entirely secure, as loopholes sometimes exist without ones knowledge, which can be exploited by the attacker. Therefore it is always advisable to keep software updated such as the embedded software on the routers in a network. Another point to be kept in mind is that the network must be tested against attacks in a closed environment to help make it resilient to potential and harmful DoS attacks. This will ensure a safer networking environment on the Internet on the whole.

REFERENCES

1. Gu, Q., Liu, P., (2008), Denial of Service Attacks, in Handbook of Computer Networks, Hossein Bidgoli et al. (eds.), John Wiley & Sons, Hoboken, NJ.
2. Aad, I., Hubaux, J.P., and Knightly E. (2004), Denial of service resilience in ad hoc networks. Proceedings of ACM Mobicom. ACM Press, New York.
3. Hussain, A., Heidemann, J. and Papadopoulos, C. (2003), A framework for classifying denial of service attacks. In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. SIGCOMM '03. ACM, New York.
4. Constantin, L. (2012), “Denial-of-service Attacks Are on the Rise, Anti-DDoS Vendors Report”, IDG News Services and Prolexic.
5. Bellardo, J., and Savage, S. (2003) 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. Proceedings of USENIX Security Symposium, 15-28. USENIX Press, Berkeley, CA.
6. Mirkovic, J., Dietrich, S., Dittrich, D. and Reiher, P. (2005) Internet Denial of Service: Attack and Defense Mechanisms, ISBN-10: 0131475738, ISBN-13: 97801314757312005, Prentice Hall.
7. Mohammed, L.A. and Isaac, B., (2006), Detailed DoS Attacks in Wireless Networks and Countermeasures, Int. J. Ad Hoc and Ubiquitous Computing, Vol 2, No. 1.
8. http://www.studymode.com/essays/Information-Technology-Information-System-1325002.html
9. http://dbpedia-live.openlinksw.com/page/The_Spamhaus_Project
10. http://www.cisco.com/warp/public/707/newsflash.html
11. http://cio.cisco.com/warp/public/707/3.html
12. http://cio.cisco.com/warp/public/707/4.html